(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109428867 B
(45)授权公告日 2020.08.25

(21)申请号 201710763841.1

(22)申请日 2017.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 109428867 A

(43)申请公布日 2019.03.05

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 吴华佳 程志军 赖朝辉

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 102843235 A,2012.12.26,
CN 106788989 A,2017.05.31,
CN 101262405 A,2008.09.10,
CN 101471784 A,2009.07.01,
CN 105071987 A,2015.11.18,
CN 102075427 A,2011.05.25,
US 7298847 B2,2007.11.20,
US 2015033014 A1,2015.01.29,
US 2004258078 A1,2004.12.23,
Xiangyang Zhang et al.IPsec anti-replay algorithm without bit-shifting.《IETF draft-zhang-ipsecme-anti-replay-07》.2011,
从延奇.IPSEC的抗重放原理及其实现.《湖南工程学院学报》.2003,

审查员 李星星

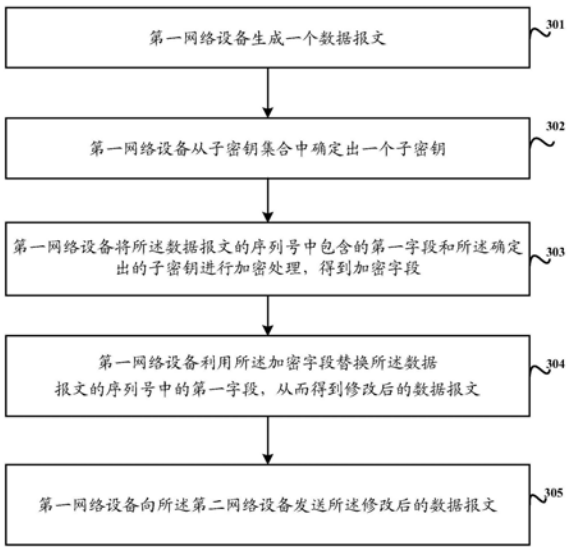
权利要求书3页 说明书13页 附图7页

(54)发明名称

一种报文加解密方法、网路设备及系统

(57)摘要

一种报文加解密方法、网路设备及系统，该方法包括：第一网络设备与第二网络设备预先协商确定原始密钥，然后第一网络设备利用原始密钥生成子密钥集合，进而从子密钥集合中确定出一个子密钥，并利用这个子密钥与自身生成的数据报文的序列号的第一字段进行加密处理，从而生成加密字段，第一网络设备利用这个加密字段替换该序列号的第一字段，然后得到修改后的数据报文，将修改后的数据报文发送至第二网络设备，因为数据报文中的序列号被加密了，所以攻击者即使截取了数据报文也无法解密得到原始序列号，因而有效地预防重放攻击的问题。



CN 109428867 B

1.一种报文加密方法,其特征在于,该方法包括:

第一网络设备生成一个数据报文;

所述第一网络设备从子密钥集合中确定出一个子密钥,所述子密钥集合包含M个子密钥,所述M个子密钥是根据原始密钥拆分得到的N个字段生成的,所述原始密钥是所述第一网络设备与第二网络设备预先协商确定的,M大于等于N;

所述第一网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理,得到加密字段,其中,所述序列号中包含多个字段;

所述第一网络设备利用所述加密字段替换所述数据报文的序列号中的第一字段,从而得到修改后的数据报文;

所述第一网络设备向所述第二网络设备发送所述修改后的数据报文。

2.根据权利要求1所述的方法,其特征在于,所述子密钥集合还包括每个子密钥对应的索引值,所述第一网络设备从子密钥集合中确定出一个子密钥,包括:

所述第一网络设备将所述序列号中包含的第二字段对M取模得到模值;

所述第一网络设备以所述模值作为索引值,从所述子密钥集合中查找到所述索引值对应的子密钥。

3.根据权利要求1或2所述的方法,其特征在于,所述第一网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理,得到加密字段,包括:

所述第一网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作,得到加密字段,其中,所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

4.根据权利要求1至2任一项所述的方法,其特征在于,所述第一网络设备从子密钥集合中确定出第一子密钥之前,还包括:

所述第一网络设备向所述第二网络设备发送因特网密钥交换IKE协商请求报文,所述IKE协商请求报文中的预定标识位的值被设置为第一值,所述第一值指示支持对序列号加密传输;

所述第一网络设备接收所述第二网络设备发送的IKE协商响应报文,所述IKE协商响应报文中的预定标识位的值被设置为所述第一值;

所述第一网络设备根据所述IKE协商响应报文中的预定标识位的值确定所述第二网络设备支持对序列号加密传输。

5.一种报文解密方法,其特征在于,该方法包括:

第二网络设备接收第一网络设备发送的数据报文;

所述第二网络设备从子密钥集合中确定出一个子密钥,所述子密钥集合包含M个子密钥,所述M个子密钥是根据原始密钥拆分得到的N个字段生成的,所述原始密钥是所述第一网络设备与所述第二网络设备预先协商确定的,M大于等于N;

所述第二网络设备将接收到的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理,得到解密字段,其中,所述序列号中包含多个字段;

所述第二网络设备利用所述解密字段替换所述数据报文的序列号中的第一字段,从而得到解密后的数据报文。

6.根据权利要求5所述的方法,其特征在于,所述子密钥集合还包括每个子密钥对应的

索引值，所述第二网络设备从子密钥集合中确定出一个子密钥，包括：

所述第二网络设备将所述数据报文的序列号中包含的第二字段对M取模得到模值；

所述第二网络设备以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

7.根据权利要求5或6所述的方法，其特征在于，所述第二网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理，得到解密字段，包括：

所述第二网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到解密字段，其中，所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

8.根据权利要求5至6任一项所述的方法，其特征在于，所述第二网络设备从子密钥集合中确定出第一子密钥之前，还包括：

所述第二网络设备接收所述第一网络设备发送的因特网密钥交换IKE协商请求报文，所述IKE协商请求报文中的预定标识位的值被设置为第一值，所述第一值指示支持对序列号加密传输；

如果所述第二网络设备支持对序列号加密传输，则所述第二网络设备向所述第一网络设备发送IKE协商响应报文，其中，所述IKE协商响应报文中的所述预定标识位的值被设置为所述第一值。

9.一种第一网络设备，其特征在于，该第一网络设备包括：通信接口、处理器以及存储器；

所述处理器调用存储在所述存储器中的指令，执行以下处理：

生成一个数据报文；

从子密钥集合中确定出一个子密钥，所述子密钥集合包含M个子密钥，所述M个子密钥是根据原始密钥拆分得到的N个字段生成的，所述原始密钥是所述第一网络设备与第二网络设备预先协商确定的，M大于等于N；

将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理，得到加密字段，其中，所述序列号中包含多个字段；

利用所述加密字段替换所述数据报文的序列号中的第一字段，从而得到修改后的数据报文；

通过所述通信接口向所述第二网络设备发送所述修改后的数据报文。

10.根据权利要求9所述的网络设备，其特征在于，所述处理器具体用于：

将所述序列号中包含的第二字段对M取模得到模值；

以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

11.根据权利要求9或10所述的网络设备，其特征在于，所述处理器具体用于：

将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到加密字段，其中，所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

12.根据权利要求9至10任一项所述的网络设备，其特征在于，所述处理器还用于：

通过所述通信接口向所述第二网络设备发送的因特网密钥交换IKE协商请求报文，所述IKE协商请求报文中的预定标识位的值被设置为第一值，所述第一值指示支持对序列号加密传输；

通过所述通信接口接收所述第二网络设备发送的IKE协商响应报文,所述IKE协商响应报文中的预定标识位的值被设置为所述第一值;

根据所述IKE协商响应报文中的预定标识位的值确定所述第二网络设备支持对序列号加密传输。

13.一种第二网络设备,其特征在于,该第二网络设备包括:通信接口、处理器以及存储器;

所述处理器调用存储在所述存储器中的指令,执行以下处理:

通过所述通信接口接收第一网络设备发送的数据报文;

从子密钥集合中确定出一个子密钥,所述子密钥集合包含M个子密钥,所述M个子密钥是根据原始密钥拆分得到的N个字段生成的,所述原始密钥是所述第一网络设备与所述第二网络设备预先协商确定的,M大于等于N;

将接收到的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理,得到解密字段,其中,所述序列号中包含多个字段;

利用所述解密字段替换所述数据报文的序列号中的第一字段,从而得到解密后的数据报文。

14.根据权利要求13所述的网络设备,其特征在于,所述处理器具体用于:

将所述数据报文的序列号中包含的第二字段对M取模得到模值;

以所述模值作为索引值,从所述子密钥集合中查找到所述索引值对应的子密钥。

15.根据权利要求13或14所述的网络设备,其特征在于,所述处理器具体用于:

将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作,得到解密字段,其中,所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

16.根据权利要求13至14任一项所述的网络设备,其特征在于,

通过所述通信接口接收所述第一网络设备发送的因特网密钥交换IKE协商请求报文,所述IKE协商请求报文中的预定标识位的值被设置为第一值,所述第一值指示支持对序列号加密传输;

如果支持对序列号加密传输,则通过所述通信接口向所述第一网络设备发送IKE协商响应报文,其中,所述IKE协商响应报文中的所述预定标识位的值被设置为所述第一值。

17.一种通信系统,其特征在于,包括执行上述权利要求9至12任一项所述的第一网络设备,以及执行上述权利要求13至16任一项所述的第二网络设备。

一种报文加解密方法、网路设备及系统

技术领域

[0001] 本申请涉及信息技术领域，尤其涉及一种报文加解密方法、网路设备及系统。

背景技术

[0002] 目前，随着网络通信在越来越多的政府部门和企业机构的广泛应用，共享信息与网上业务的不断增加，网络攻击和犯罪活动猖獗。如何防止网络中机密信息的泄露和篡改、阻止与打击信息犯罪、保障网络与信息安全，给人们提出了严峻的挑战。网络通信每天都面临着大量的各种方式的攻击，攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息，如修改、删除、伪造、添加、重放、乱序冒充等。被动攻击是指在不干扰网络系统正常工作的情况下，进行侦收、截获、窃取、破译等。其中，重放是一种重要的攻击手段。

[0003] 重放攻击是指攻击者首先通过网络截取通信对等双方正常通信的数据包，然后将数据包原封不动，或经过修改，在等待一段时间之后，再发给数据包的接收者，即“重放”。重放的目的是为了冒充合法的一方和另一方进行通信。之所以采用重放的方式而不是直接发送伪造的数据包，是因为有的系统会将部分信息进行加密和认证，伪造的数据包可能无法取得数据包接收方的信任，而采用重放原本合法的数据包则可以达到此目的。

[0004] 现有技术为了解决重放攻击的问题，在每个安全性网络协议(internet protocol security，IPSec)报头内，都包含了一个独一无二、且单调递增的序列号，通过每个数据包的序列号和一个“滑动”的接收窗口来主动筛选出重放报文，但是由于序列号单调递增，易猜测，容易造成防重放机制失效。

发明内容

[0005] 有鉴于此，本申请提供了一种报文加解密方法、网络设备及系统，用以解决有效地预防重放攻击的问题。

[0006] 第一方面，本申请实施例提供了一种报文加密方法，该方法包括：第一网络设备与第二网络设备预先协商确定原始密钥，然后第一网络设备利用原始密钥生成子密钥集合，进而从子密钥集合中确定出一个子密钥，并利用这个子密钥与生成的数据报文的序列号的第一字段进行加密处理，从而生成加密字段，第一网络设备利用这个加密字段替换该数据报文的序列号的第一字段，然后得到修改后的数据报文，将修改后的数据报文发送至第二网络设备。

[0007] 因为数据报文中的序列号被加密了，所以攻击者即使截取了数据报文也无法解密得到原始序列号，所以可以有效地预防重放攻击的问题。

[0008] 其中，第一网络设备与第二网络设备预先协商确定原始密钥的方式主要是采用IKE协商，协商过程是第一网络设备向所述第二网络设备发送因特网密钥交换IKE协商请求报文，其中IKE协商请求报文中的预定标识位的值指示第一网络设备支持对序列号加密传输；然后第二网络设备向第一网络设备发送IKE协商响应报文，其中，IKE协商响应报文中的

预定标识位的值指示所述第二网络设备支持对序列号加密传输，并且在协商过程中利用密钥种子生成一个原始密钥。

[0009] 进而，第一网络设备将与所述第二网络设备协商确定的原始密钥拆分为N个字段，然后将所述N个字段复制成M个字段，并生成由M个字段组成的子密钥集合，之所以这样做，是为了增加子密钥的随机性和复杂性，避免被攻击者猜测出来。

[0010] 在一种可能的设计中，第一网络设备从子密钥集合中确定出一个子密钥的方法可以是第一网络设备将所述数据报文的序列号中包含的第二字段对M取模得到模值；然后以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。这样做的好处是序列号不同所以取模对应的模值也不相同，故确定出的子密钥也是动态的，所以攻击者很难破解得到子密钥，因此提高了加密方法的可靠性。

[0011] 其中，第一网路设备对数据报文的加密方法有多种，在一种可能的设计中，第一网络设备将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到加密字段。一般，为了保证数据报文的长度尽可能不变，子密钥的字节数目一般与第一字段的数目相同。如果数据报文长度变长会增大开销，若变短则容易被攻击者破解，需要说明的是，上述加密方法也可以采用同或替代，即将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行同或操作，得到加密字段。相比而言，异或加密方式，不用像同或操作在解密时先取反，因此解密过程相对简便一些。

[0012] 另外，上面第一字段可以是序列号的高位字节部分，也可以是低位字节部分，假设说序列号包括L个字节，那么第一字段可以为所述序列号L/2个字节的高位字节部分，第二字段则为所述序列号L/2个字节的低位字节部分；或者所述第一字段可以为所述序列号L/2个字节的低位字节部分，则第二字段为所述序列号L/2个字节的高位字节部分。

[0013] 第二方面，与上面加密方法相对应，本发明实施例进一步地提供一种报文解密方法，该方法包括第二网络设备在接收到第一网络设备发送的数据报文之后，按照与第一网络设备相同的方式确定出一个子密钥，然后利用该子密钥对接收到的数据报文中序列号进行解密，解密方法与加密方法相对应，即将接收到的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理，得到解密字段，再利用所述解密字段替换所述数据报文的序列号中的第一字段，从而得到解密后的报文。

[0014] 这样即使数据报文中的序列号被加密了，第二网络设备可以按照解密方法对其进行正确解密，得到原始序列号，而攻击者即使截取了数据报文也无法解密得到原始序列号，所以可以有效地预防重放攻击的问题。

[0015] 当然，第二网络设备预先执行了与第一网络设备的IKE协商过程，协商过程与上文一致，因此该处不再赘述。另外，生成子密钥集合的方式以及从子密钥集合中确定出子密钥的过程也与上文相一致。

[0016] 第二网路设备对报文的解密方法是与加密方法相对应的，在一种可能的设计中，若第一网络设备采用的加密操作是异或，那么第二网络设备将接收到的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到解密字段；在另一种可能的设计中，若第一网络设备采用的加密操作是同或，那么第二网络设备将接收的序列号先取反，然后将接收的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，就可以得到解密字段。相比而言，异或加密方式，不用像同或操作在解密时先取反，因此

解密过程相对简便一些。

[0017] 第三方面，本申请实施例还提供了一种网络设备，该网络设备具有实现上述第一方面方法示例中报文加密行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或所述软件包括一个或多个与上述功能相对应的模块。

[0018] 在一个可能的设计中，所述网络设备的结构中包括确定单元、加密单元、处理单元、发送单元，这些单元可以执行上述方法示例中相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0019] 第四方面，本申请实施例还提供了一种第一网络设备，该第一网络设备具有实现上述第一方面方法示例中报文加密行为的功能。所述功能可以通过硬件实现。所述第一网络设备的结构中包括通信接口、处理器、以及存储器，其中，所述处理器调用存储在所述存储器中的指令，执行以下处理：

[0020] 从子密钥集合中确定出一个子密钥，将生成的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理，得到加密字段，并利用所述加密字段替换所述数据报文的序列号中的第一字段，从而得到修改后的数据报文；然后通过所述通信接口将包含所述序列号密文的数据报文发送至所述第二网络设备。

[0021] 因为数据报文中的序列号被加密了，所以攻击者即使截取了数据报文也无法解密得到原始序列号，所以可以有效地预防重放攻击的问题。

[0022] 其中，第一网络设备与第二网络设备预先协商确定原始密钥的方式主要是采用IKE协商，协商过程是，在确定子密钥之前，所述处理器还用于：通过所述通信接口向所述第二网络设备发送的因特网密钥交换IKE协商请求报文，所述IKE协商请求报文中的预定标识位的值为第一值，其中第一值指示支持对序列号加密传输；通过所述通信接口接收所述第二网络设备发送的IKE协商响应报文，其中IKE协商响应报文中的预定标识位也是第一值的情况下，处理器确定所述第二网络设备支持对序列号加密传输。并且在协商过程中利用密钥种子生成一个原始密钥。

[0023] 进而，处理器将与所述第二网络设备协商确定的原始密钥拆分为N个字段；将所述N个字段复制成M个字段，并生成由M个字段组成的子密钥集合。之所以这样做，是为了增加子密钥的随机性和复杂性，避免被攻击者猜测出来。

[0024] 在一种可能的设计中，处理器将所述序列号中包含的第二字段对M取模得到模值；然后以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

[0025] 其中，对报文的加密方法有多种，在一种可能的设计中，处理器将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到加密字段。一般，为了保证数据报文的长度尽可能不变，子密钥的字节数目一般与第一字段的数目相同。

[0026] 另外，上面第一字段可以是序列号的高位字节部分，也可以是低位字节部分，假设说序列号包括L个字节，那么第一字段可以为所述序列号L/2个字节的高位字节部分，第二字段则为所述序列号L/2个字节的低位字节部分；或者所述第一字段可以为所述序列号L/2个字节的低位字节部分，则第二字段为所述序列号L/2个字节的高位字节部分。

[0027] 第五方面，本申请实施例还提供了一种第二网络设备，该第二网络设备具有实现上述第二方面方法示例中报文解密行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或所述软件包括一个或多个与上述功能相对应的模

块。

[0028] 在一个可能的设计中，所述第二网络设备的结构中包括确定单元、接收单元、解密单元、处理单元，这些单元可以执行上述方法示例中相应功能，具体参见方法示例中的详细描述，此处不做赘述。

[0029] 第六方面，本申请实施例还提供了一种第二网络设备的另一种结构，该第二网络设备具有实现上述第二方面方法示例中报文解密行为的功能。所述功能可以通过硬件实现。所述网络设备的结构中包括通信接口、处理器、以及存储器，其中，所述处理器和所述存储器通过总线连接；所述处理器调用存储在所述存储器中的指令，执行上述方法，该处不再赘述。

[0030] 第七方面，本申请实施例中还提供一种计算机存储介质，该存储介质中存储软件程序，该软件程序在被一个或多个处理器读取并执行时可实现第一方面或上述第一方面的任意一种设计提供的方法。

[0031] 第八方面，本申请实施例中还提供一种计算机存储介质，该存储介质中存储软件程序，该软件程序在被一个或多个处理器读取并执行时可实现第二方面或上述第二方面的任意一种设计提供的方法。

[0032] 第九方面，本申请还提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述各方面或各种可能的实现方式所述的报文加密方法。

[0033] 第十方面，本申请还提供了一种计算机程序，当其在计算机上运行时，使得计算机执行上述各方面或各种可能的实现方式所述的报文解密方法。

[0034] 本申请中，因为子密钥在第一网络设备和第二网络设备之间协商确定的加密通道中传输，且是动态变化的，所述加密后的数据报文安全性高，另外对序列号进行加密的子密钥通过取模的方式确定，所以随机性高，加密后的序列号不可猜测，因此可以有效地防止重放攻击。

附图说明

[0035] 图1为本申请实施例提供的一种系统架构示意图；

[0036] 图2为本申请实施例提供的一种基于IKE协商的系统架构示意图；

[0037] 图3为本申请实施例提供的一种报文加密方法的流程示意图；

[0038] 图4为本申请实施例提供的IKE协商交互示意图；

[0039] 图5a～图5b为本申请实施例提供的报文保留字段位置示意图；

[0040] 图6为本申请实施例提供的一种报文解密方法的流程示意图；

[0041] 图7为本申请实施例提供的一种网路设备的装置示意图一；

[0042] 图8为本申请实施例提供的一种网路设备的装置示意图二；

[0043] 图9为本申请实施例提供的一种网路设备的结构示意图。

具体实施方式

[0044] 下面将结合附图对本申请作进一步地详细描述。

[0045] 本申请中的报文加解密方法可适用于多种系统架构，图1为本申请适用的一种系统架构示意图。如图1所示，该系统架构中包括：发送端服务器101、发送端网关102、接收端

网关103、接收端服务器104。

[0046] 其中，为了保证发送端网关102和接收端网关103传输数据包的安全性，发送端网关102和接收端网关103之间采用IPSec协议传输报文。

[0047] 需要说明的是，IPSec是国际互联网工程任务组(the internet engineering task force，IETF)制定的为保证在因特网上传送数据的安全保密性能的三层隧道加密协议。IPSec在网络层(internet protocol，IP)对IP报文提供安全服务。IPSec协议本身定义了如何在IP数据包中增加字段来保证IP数据包的完整性、私有性和真实性，以及如何加密数据包。使用IPsec，数据就可以安全地在公网上传输。IPsec提供了两个主机之间、两个安全网关之间或主机和安全网关之间的保护。

[0048] IPSec包括报文验证头协议(authentication header，AH)(协议号51)和报文安全封装协议(encapsulated security payload，ESP)(协议号50)两个协议。AH可提供数据源验证和数据完整性校验功能；ESP除可提供数据验证和完整性校验功能外，还提供对IP报文的加密功能。IPSec协议的安全特点是1、数据机密性，即IPSec发送方在通过网络传输包前对包进行加密。2、数据完整性，即IPSec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。3、数据来源认证，即IPSec接收方对IPSec包的源地址进行认证。这项服务基于数据完整性服务。4、反重放攻击，即IPSec接收方可检测并拒绝接收过时或重复的报文。

[0049] 所谓重放攻击是指攻击者首先通过网络截取通信对等双方正常通信的数据包，然后将数据包原封不动，或经过修改，在等待一段时间之后，再发给数据包的接收者，即“重放”。重放的目的是为了冒充合法的一方和另一方进行通信。之所以攻击者采用重放的方式而不是直接发送伪造的数据包，是因为有的系统会将部分信息进行加密和认证，伪造的数据包可能无法取得数据包接收方的信任，而采用重放原本合法的数据包则可以达到此目的。比如说，在移动IP中，当移动节点发现它的网络从一条链路切换到另一条链路上的时候，就要进行注册。注册的目的，一方面可以使移动节点得到外地链路上的外地代理的路由服务，另一方面可以通知家乡代理移动节点转交地址。注册消息是一个用户数据报协议(User Datagram Protocol，UDP)数据包，包含在IP数据包内。如果有攻击者截取了这个数据包，然后修改转交地址字段，然后再重发这个消息，则攻击者便注册到了一个伪造的转交地址。那么以后网络中所有发送给移动节点的数据包都会被转发到攻击者注册的那个转交地址那里，移动节点再也不会收到任何信息了。

[0050] 虽然利用IPSec协议传输报文，接收方可检测并拒绝接收过时或重复的报文，一定程度上可以防止重放攻击，但是因为IPSec协议传输的报文的序列号是明文，序列号具有单调递增或者递减的特点，所以攻击者一旦截取了一个报文，很容易根据该报文的序列号猜测后续报文的序列号，进而冒充发送方与接收方进行通信，而接收方单纯通过解析序列号，如果判断不是重复或者过时的，就会认为报文是合法的，所以无法准确地识别出攻击者的非法报文，这样容易造成IPSec协议的防重放作用失效。

[0051] 现有技术中也有新增校验字段对报文的序列号进行额外的校验方式，这样攻击者可以获取有效的序列号，但是无法通过报文验证，但是这样做的缺点是由于在报文头中新增了字段，所以需要调整报文的长度，带来额外的开销较大。

[0052] 考虑到现有IPSec报文还包含因特网密钥交换(internet key exchange，IKE)协

议,IKE协商的主要功能是通信双方实现密钥协商,通过协商过程可以验证通信双方的身份是否合法,并在合法的情况下建立IPsec安全联盟(Security Association,SA)。基于上述原因,本申请实施例提供一种报文加解密方法,该方法结合利用了IKE协商机制,通过采用IKE协商确定的密钥种子,生成密钥,并利用该密钥将明文的序列号加密成密文,这样攻击者因为无法破解密钥,所以攻击者即使截取了数据报文,也无法猜测出后续的序列号,因此可以有效地预防重放攻击。

[0053] 详细来说,IPSec报文所包含的IKE协议其主要功能就是在不安全的网络上安全地协商、分发、管理密钥、验证身份、建立安全联盟。SA是通信双方达成的一个协定,只有知道协定的全部信息,才能进行正确的IPSec处理。例如,协定好使用ESP方式进行封装,就不能使用AH方式进行解封装;同样,协定好使用3DES加密,就不能使用AES方式解密。

[0054] 为确保顺利进行IPSec通信,IKE协议执行双阶段协商。这两个阶段分别是主模式(Main Mode)协商和快速模式(Quick Mode)协商。

[0055] 1、主模式(也称为第1阶段)IKE协商在两台计算机之间建立一个称为ISAKMP SA的安全通道。该安全通道主要是用于保护安全协商。

[0056] 2、快速模式(也称为第2阶段)IKE协商在两台计算机之间建立一个通道来保护数据。由于这个阶段涉及SA的创建,因此在快速模式期间建立的SA称为IPSec SA。在快速模式期间,加密材料将被刷新,或在必要时生成新的密钥。在此期间还会选择一个用于保护特定IP流量的保护套件。

[0057] 通过上述协商后可以生成一个共享密钥材料即密钥种子(SKEYSEED)。密钥种子的计算公式如下:

[0058] SKEYSEED＝prf(Ni|Nr,g^ir)……….公式[1]

[0059] SKEYSEED＝{SK_d|SK_ai|SK_ar|SK_ei|SK_er|SK_pi|SK_pr}

[0060] ＝prf+(SKEYSEED,Ni|Nr|SPIi|SPIr)……公式[2]

[0061] 其中,SK_d用于第二阶段扩展密钥(只有它是不分方向的),SK_ai和SK_ar分别用作发起方和响应方的MAC密钥,SK_ei和SK_er分别用作发起方和响应方的加密密钥,SK_pi和SK_pr用于发起方和响应方的认证载荷计算。

[0062] 另外,通过上述协商,双方可以根据协商结果确定后续在收到对方发送的数据报文时,是否需要进行解密,比如,协商结果是对方不支持加密,那么发送方就不会对待发送的数据报文加密,而是直接向接收侧发送,同时接收侧收到数据报文不进行解密操作,而是直接获取序列号进行校验。当然,如果协商结果是对方支持加密,那么发送方就会对待发送的数据报文加密,然后将加密后的数据报文发送至接收侧,同时接收侧收到数据报文进行解密操作。

[0063] 具体来说,本申请实施例提供的报文加解密方法包括报文加密方法和报文解密方法,适用本申请实施例提供的报文加解密方法的通信系统如图2所示,图2中主要包含如下过程:发送端网关102和接收端网关103之间先建立IKE的SA协商,然后发送端网关102利用协商确定的加密算法对IPSec报文进行加密,生成加密后的IPSec报文,然后将加密后的IPSec报文发送至接收端网关103,其中,接收端网关103用协商确定的解密算法对加密后的数据报文解密,还原得到原始的IPSec报文的序列号。

[0064] 下文拆解为加密过程和解密过程这两个过程分别对其进行详细阐述。

[0065] 如图3所示，本申请实施例提供的一种报文加密方法的流程示意图，具体步骤如下：

[0066] 步骤301，第一网络设备生成一个数据报文。

[0067] 步骤302，所述第一网络设备从子密钥集合中确定出一个子密钥。例如，第一网络设备可以是附图2中的发送端网关102。

[0068] 步骤303，所述第一网络设备将待发送报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理，得到加密字段。

[0069] 步骤304，所述第一网络设备利用所述加密字段替换所述数据报文的序列号中的第一字段，从而得到修改后的数据报文。

[0070] 步骤305，所述第一网络设备向第二网络设备发送所述修改后的数据报文。例如，第二网络设备可以是附图2中的接收端网关103。

[0071] 需要说明的在执行步骤301之前，第一网络设备需要确定对端的第二网络设备是支持加密传输的，也就是说，第二网络设备接收到加密后的数据报文可以对其进行解密。因此在执行步骤301之前，第一网络设备和第二网络设备之间需要先进行IKE协商过程，协商的交互示意图如图4所示，包括：

[0072] 步骤401，第一网络设备向所述第二网络设备发送IKE协商请求报文。

[0073] 步骤402，第一网络设备接收所述第二网络设备发送的IKE协商响应报文。

[0074] 其中，第一网络设备发送的IKE协商请求报文携带预定标识位，而且预定标识位为第一值，第一值指示第一网络设备支持对序列号的加密传输，如果第二网络设备也支持对序列号的加密传输，则第二网络设备反馈的IKE协商响应报文中也携带该预定标识位，且预定标识为的值也为第一值。这样，第一网络设备根据所述IKE协商响应报文中的标识位的第一值可以确定所述第二网络设备支持对序列号加密传输。

[0075] 当第一网络设备确定对端的第二网络设备支持加密传输后，则第一网络设备对数据报文执行上述图3所述的加密过程，然后向第二网络设备发送加密后的数据报文；否则，第一网络设备省略加密过程，直接向第二网络设备发送未加密的数据报文。这样做可以兼容不支持加密传输的网络设备，避免发生通信失败的问题。

[0076] 其中，第一网络设备和第二网络设备所采用的标识位是IKE报文中未被使用的保留字段，例如，第一网络设备使用Security Association payload(安全联盟负载)头中RESERVED(保留字段)的7bit中的第一bit来标识第一网络设备是否支持对序列号进行加密，在整个Payload(负载)头中占位为第10bit。如图5a所示，E表示所使用的标识位，该标识位的值为0表示不支持对序列号进行加密，该标识位的值为1表示支持对序列号进行加密。这样，当第二网络设备收到该IKE协商请求报文，对Security Association payload(安全联盟负载)头中RESERVED(保留字段)中的第一bit进行解析判断，如果值为1，则认为第一网络设备支持对数据报文加密，后续在收到第一网络设备发送的数据报文时，首先对其进行解密操作。

[0077] 另外，也可以如图5b所示，E表示所使用的标识位，值为0表示不支持对序列号进行加密，值为1表示支持对序列号进行加密。第二网络设备收到IKE协商请求报文，判断负荷中的标识位的值，如果值为1，则认为第一网络设备支持对数据报文加密，后续在收到第一网络设备发送的数据报文时，首先对其进行解密操作。

[0078] 另外，当第一网络设备与对端的第二网络设备完成IKE协商，确定对端支持加密传输之后，第一网络设备首先利用协商确定的密钥种子公式，生成原始密钥，再利用原始密钥生成子密钥集合。具体地，所述第一网络设备将与所述第二网络设备协商确定的原始密钥拆分为N个字段；然后所述第一网络设备将所述N个字段复制成M个字段，进而生成由M个字段组成的子密钥集合，一般M会大于N。

[0079] 例如说，将表一中的原始密钥Key值拆分为8个2字节，将这8个2字节按照值从大到小的顺序排列，依次循环填满一个长度为100的表二所示的Key表。

[0080] 表一

[0081]

0x2fe0	0x1fd9	0x1ee1	0x1fe5	0x1fa0	0x11a1	0x21c3	0x1fe9

[0082] 表二

[0083]

0x2fe0	0x21c3	0x1fe9	0x1fe5	0x1fd9	0x1fa0	0x1ee1
……	0x1fe5	0x1fd9	0x1fa0	0x1ee1		

[0084] 另外，将表一中的原始密钥Key值拆分为8个2字节之后，也可以对表一中每个2字节进行变形，再用变形后的2字节生成Key表，变形方法可以是加1，或者其它现有方法，在此不再赘述。

[0085] 在一种可能的设计中，第一网络设备从子密钥集合中确定出一个子密钥，确定方法可以是所述第一网络设备将数据报文的序列号中包含的第二字段对M取模得到模值；所述第一网络设备以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

[0086] 比如说，将序列号0xefac 0x1b21的低16位0x1b21对M(例如M为100)取模，得到模值45，查找表二中Key表中第45个子密钥0x1fd9。当然，除此之外，也可以在IKE协商阶段，第一网络设备和第二网络设备协商指定子密钥集合某一个索引号为子密钥，比如说指定表二中KEY表中的第45个值0x1fd9作为子密钥。显然，利用取模方式可以更加动态地确定出子密钥，不容易被攻击者破解。

[0087] 当确定出子密钥之后，就可以利用确定出来的子密钥对序列号进行加密，在一种可能的设计中，第一网络设备将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到加密字段。例如，将子密钥0x1fd9与序列号的高16位0xefac进行异或操作，得到新的加密值0xf075，用新的加密值0xf075替换序列号的高16位0xefac后得到新的序列号0xf075 0x1b21，用新的序列号0xf075 0x1b21替换原数据报文中的序列号，将替换之后的数据报文发送至对端第二网络设备。这样，第二网络设备仍然采用异或操作就可以还原出原序列号，解密算法也很简便。

[0088] 一般，为了保证数据报文的长度尽可能不变，子密钥的字节数目一般与第一字段的数目相同。一方面，便于进行异或操作，另一方面数据报文长度变长会增大开销，若变短则容易被攻击者破解。需要说明的是，上述加密方法也可以采用同或替代，即将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行同或操作，得到加密字段。相比异或加密方式，采用同或操作，第二网络设备在解密时就需要先取反，再进行异或操作，解密过程相对复杂一些。

[0089] 上面例子中，第一字段是序列号的高16位0xefac，第二字段是低16位0x1b21，需要说明的是，在其它可能的设计中，第一字段也可以不是序列号的一半字节，例如序列号是4

字节，第一字段是1字节部分，第二字段是3字节部分，这样划分也可以实现上述方法，即对第二字段取模确定子密钥，然后进行加密运算。同样地，上面例子中，第一字段也可以是序列号的低16位0x1b21，第二字段是高16位0xefac，即对高16位取模，得到模值，然后低16位与模值对应的密钥值进行加密运算。

[0090] 与上述报文加密方法相对应，本申请实施例进一步对报文解密方法的具体过程进行详细说明，具体步骤如图6所示。

[0091] 步骤601，第二网络设备接收第一网络设备发送的数据报文。例如，第一网络设备可以是附图2中的发送端网关102，第二网络设备可以是附图2中的接收端网关103。

[0092] 步骤602，第二网络设备从子密钥集合中确定出一个子密钥。

[0093] 步骤602，所述第二网络设备接收所述第一网络设备发送的报文。

[0094] 步骤603，所述第二网络设备将接收的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理，得到解密字段。

[0095] 步骤604，所述第二网络设备利用所述解密字段替换所述数据报文的序列号中的第一字段，从而得到解密后的数据报文。

[0096] 与上述报文加密方法类似，第二网络设备在接收到第一网络设备发送的数据报文之前，已经与第一网络设备完了IKE协商，利用协商确定的密钥种子公式，生成原始密钥，再利用原始密钥生成子密钥集合，其中子密钥集合的生成方式与上文相同，因此此处不再赘述。

[0097] 也就是说，第二网络设备也按照与第一网络设备相同的方法，确定出子密钥集合，进一步再按照与第一网络设备一样的规则从子密钥集合中确定出一个子密钥，比如说，第一网络设备是对第二字段取模，利用模值作为索引值确定出子密钥，那么第二网络设备也是按照相同的规则确定出子密钥。

[0098] 在一种可能的设计中，所述第二网络设备将所述数据报文的序列号中包含的第二字段对M取模得到模值；所述第二网络设备以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

[0099] 比如说，仍然以序列号0xefac 0x1b21为例，在上文中，第一网络设备用表2的Key表中第45个子密钥0x1fd9对其进行加密得到新的序列号0xf075 0x1b21，那么第二网络设备收到包含该序列号0xf075 0x1b21的数据报文，仍然利用第45个子密钥0x1fd9对0xf075 0x1b21的高16位0xf075进行异或操作，将得到新的解密值0xefac，用新的解密值0xefac替换序列号的高16位0xf075后得到新的序列号0xefac 0x1b21，即还原得到第一网络设备所发送的数据报文对应的原始序列号。当然，若第一网络设备采取其它的规则确定出子密钥，并利用子密钥对序列号进行加密，例如对低位字节部分进行异或操作，得到新的加密值，这时第二网络设备也是对低位字节部分进行异或操作，得到新的解密值。

[0100] 在另一种可能的设计中，若第一网络设备将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行同或操作，得到加密字段，那么第二网络设备在解密时就需要先取反，再进行异或操作。例如，第一网络设备利用第45个子密钥0x1fd9对0xf075 0x1b21的高16位0xf075进行同或操作，那么，第二网络设备就需要先对数据报文的序列号0xf075 0x1b21先取反，然后再对取反之后的序列号按照上面的例子中的方法解密。

[0101] 针对上述方法流程，本申请提供一种网络设备，该网络设备的具体执行内容可参

照上述报文加密方法对应实施例。

[0102] 图7为本申请提供的一种第一网络设备的结构示意图，如图7所示，所述第一网络设备包括：

[0103] 生成单元701，用于生成一个数据报文。

[0104] 确定单元702，用于从子密钥集合中确定出一个子密钥，所述子密钥集合包含M个子密钥，所述M个子密钥是根据原始密钥拆分得到的N个字段生成的，所述原始秘钥是所述第一网络设备与第二网络设备预先协商确定的，M大于等于N。

[0105] 加密单元703，用于将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理，得到加密字段，其中，所述序列号中包含多个字段。

[0106] 处理单元704，用于利用所述加密字段替换所述数据报文的序列号中的第一字段，从而得到修改后的数据报文。

[0107] 发送单元705，用于向所述第二网络设备发送所述修改后的数据报文。

[0108] 可选地，所述确定单元702具体用于：将所述序列号中包含的第二字段对M取模得到模值；以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

[0109] 可选地，所述加密单元703具体用于：将数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到加密字段，其中，所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

[0110] 其中，所述序列号包括L个字节，则所述第一字段为所述序列号L/2个字节的高位字节部分，所述第二字段为所述序列号L/2个字节的低位字节部分；或者所述第一字段为所述序列号L/2个字节的低位字节部分，所述第二字段为所述序列号L/2个字节的高位字节部分。

[0111] 所述第一网络设备还包括：生成单元701，用于将与所述第二网络设备协商确定的原始密钥拆分为N个字段；将所述N个字段复制成M个字段，并生成由M个字段组成的子密钥集合。

[0112] 可选地，所述发送单元705还用于：向所述第二网络设备发送因特网密钥交换IKE协商请求报文，所述IKE协商请求报文中的标识位的值指示自身支持对序列号加密传输；

[0113] 所述网络设备还包括：接收单元706，还用于接收所述第二网络设备发送的IKE协商响应报文；

[0114] 可选地，所述确定单元702，还用于根据所述IKE协商响应报文中的标识位的值确定所述第二网络设备支持对序列号加密传输。

[0115] 图8为本申请提供的与报文解密方法相对应的第二网络设备的结构示意图，如图8所示，所述第二网络设备包括：确定单元801、接收单元802、解密单元803和处理单元804；具体地：

[0116] 接收单元801，用于接收第一网络设备发送的数据报文。

[0117] 确定单元802，用于从子密钥集合中确定出一个子密钥，所述子密钥集合包含M个子密钥，所述M个子密钥是根据原始密钥拆分得到的N个字段生成的，所述原始秘钥是第一网络设备与所述第二网络设备预先协商确定的，M大于等于N。

[0118] 解密单元803，用于将接收的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理，得到解密字段，其中，所述序列号中包含多个字段。

[0119] 处理单元804，用于利用所述解密字段替换所述数据报文的序列号中的第一字段，从而得到解密后的报文。

[0120] 可选地，所述确定单元802具体用于：将所述序列号中包含的第二字段对M取模得到模值；以所述模值作为索引值，从所述子密钥集合中查找到所述索引值对应的子密钥。

[0121] 可选地，所述解密单元803具体用于：将接收的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行异或操作，得到解密字段，其中，所述确定出的子密钥的字节数目与所述第一字段的字节数目相同。

[0122] 其中，所述序列号包括L个字节，则所述第一字段为所述序列号L/2个字节的高位字节部分，所述第二字段为所述序列号L/2个字节的低位字节部分；或者所述第一字段为所述序列号L/2个字节的低位字节部分，所述第二字段为所述序列号L/2个字节的高位字节部分。

[0123] 所述第二网络设备还包括：

[0124] 生成单元805，用于将与所述第一网络设备协商确定的原始密钥拆分为N个字段；并将所述N个字段复制成M个字段，并生成由M个字段组成的子密钥集合。

[0125] 可选地，所述接收单元802，还用于接收所述第一网络设备发送的IKE协商请求报文，所述IKE协商请求报文中的标识位的值指示所述第一网络设备支持对序列号加密传输；

[0126] 所述第二网络设备还包括：

[0127] 发送单元806，用于向所述第一网络设备发送IKE协商响应报文，其中，所述IKE协商响应报文中的所述标识位的值指示所述第二网络设备支持对序列号的加密传输。

[0128] 图9为本申请提供的另一种网络设备的结构示意图，该网络设备可以执行上述报文加密方法或者报文解密方法，如图9所示，所述网络设备900包括：通信接口901、处理器902、存储器903和总线系统904；

[0129] 其中，存储器903，用于存放程序。具体地，程序可以包括程序代码，程序代码包括计算机操作指令。存储器903可能为随机存取存储器(random-access memory，RAM)，也可能为非易失性存储器(non-volatile memory，NVM)，例如至少一个磁盘存储器。图中仅示出了一个存储器，当然，存储器也可以根据需要，设置为多个。存储器903也可以是处理器902中的存储器。

[0130] 存储器903存储了如下的元素，可执行模块或者数据结构，或者它们的子集，或者它们的扩展集：

[0131] 操作指令：包括各种操作指令，用于实现各种操作。

[0132] 操作系统：包括各种系统程序，用于实现各种基础业务以及处理基于硬件的任务。

[0133] 处理器902控制网络设备900的操作，处理器902还可以称为中央处理单元(英文：central processing unit，CPU)。具体的应用中，网络设备900的各个组件通过总线系统904耦合在一起，其中总线系统904除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统904。为便于表示，图9中仅是示意性画出。

[0134] 具体来说，如果网络设备900所执行的方法是报文加密方法，那么网络设备900就对应图2中的发送端网关102，结合图3来说，通信接口901用于执行步骤305，即向第二网络设备发送所述修改后的数据报文。如果网络设备900所执行的方法是报文解密方法，那么网

络设备900就对应图2中的接收端网关103，结合图6来说，通信接口901用于执行步骤601，即接收第一网络设备发送的数据报文。

[0135] 同样地，如果网络设备900所执行的方法是报文加密方法，那么处理器902就用于执行图3中的步骤301至步骤304。如果网络设备900所执行的方法是报文解密方法，那么处理器902就用于执行图6中的步骤602至步骤604。关于处理器902的执行细节请参考前面方法实施例中的描述，在这里不再详述。

[0136] 其中，处理器902可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器902中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器902可以是通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器903，处理器902读取存储器903中的信息，结合其硬件执行以上方法步骤。

[0137] 从上述内容可以看出：本申请实施例中，因为子密钥在第一网络设备和第二网络设备之间协商确定的加密通道中传输，且是动态变化的，所述加密后的数据报文安全性高，另外对序列号进行加密的子密钥通过取模的方式确定，所以随机性高，加密后的序列号不可猜测，因此可以有效地防止重放攻击；第一网络设备和第二网络设备仅使用未被使用的保留字段来标识自身是否对数据报文加密，因此不会增加数据报文的长度，开销并没有增加。

[0138] 本领域内的技术人员应明白，本发明实施例可提供为方法、系统、或计算机程序产品。因此，本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0139] 本发明实施例是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0140] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0141] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计

算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0142] 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本申请的范围。这样，倘若本发明实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

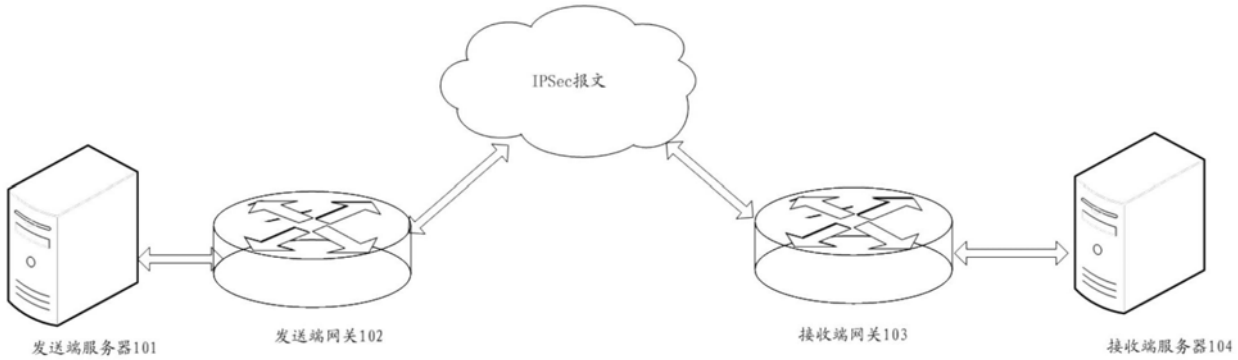

IPSec报文
发送端服务器101
发送端网关102
接收端网关103
接收端服务器104

图1

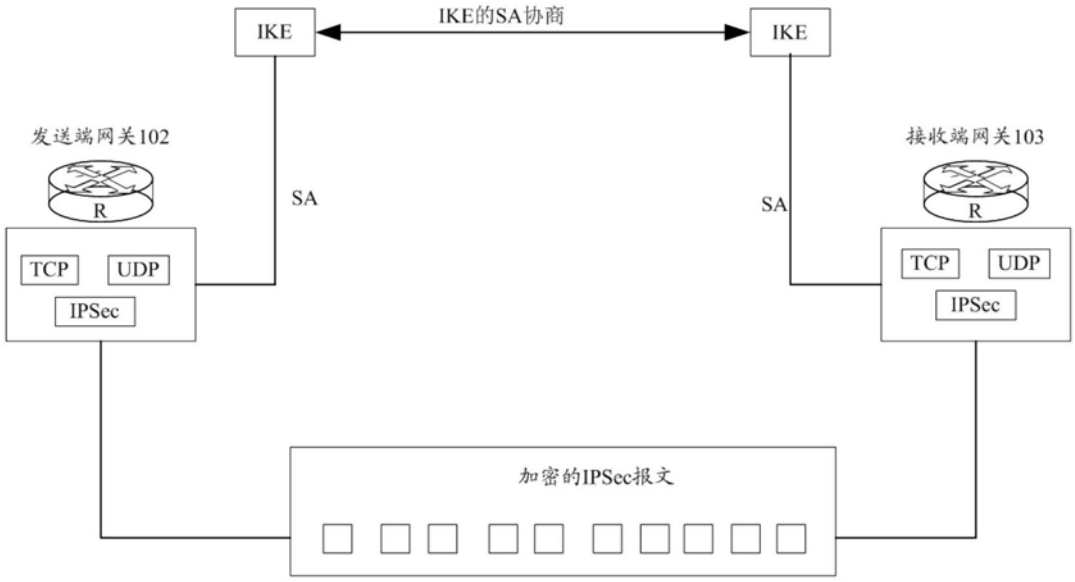

IKE
IKE的SA协商
IKE
发送端网关102
R
SA
SA
接收端网关103
R
TCP
UDP
IPSec
TCP
UDP
IPSec
加密的IPSec报文

图2

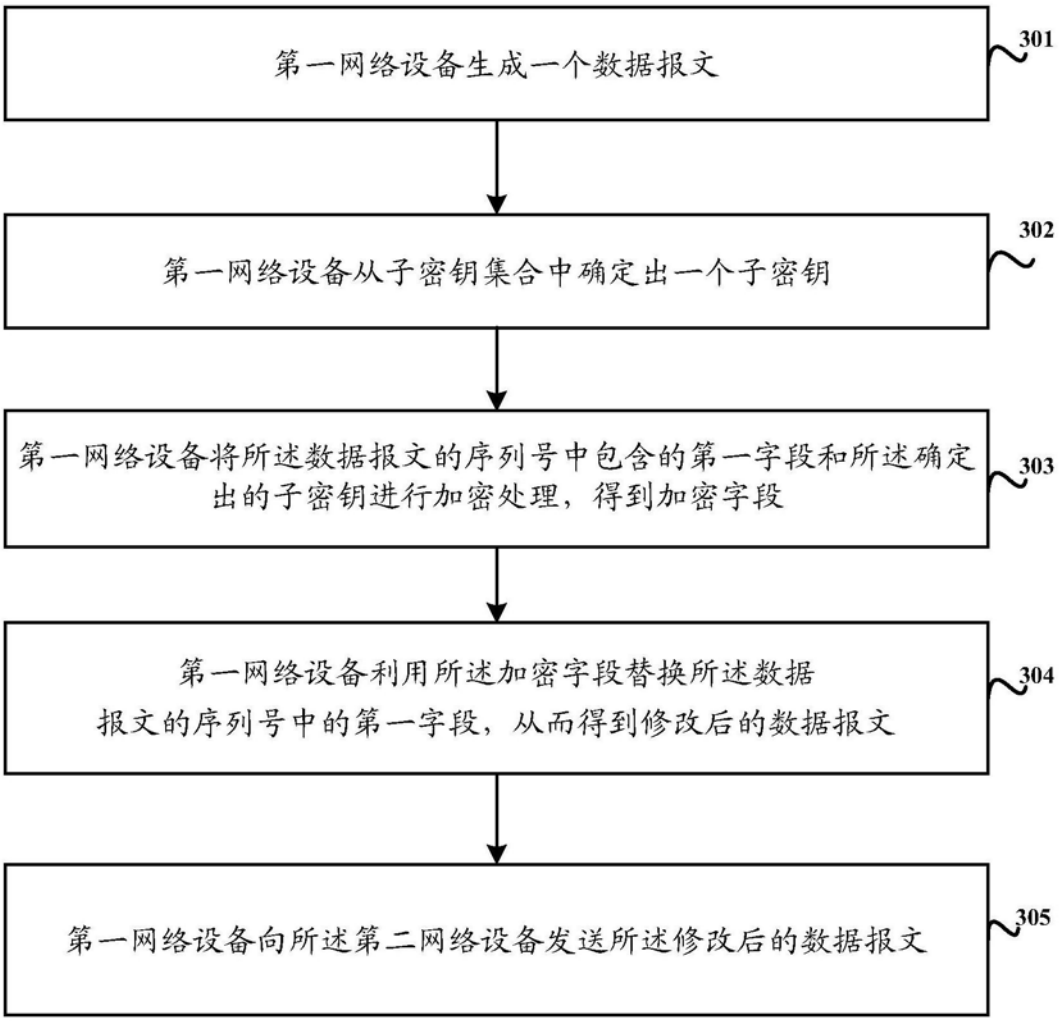

第一网络设备生成一个数据报文
301
第一网络设备从子密钥集合中确定出一个子密钥
302
第一网络设备将所述数据报文的序列号中包含的第一字段和所述确定出的子密钥进行加密处理，得到加密字段
303
第一网络设备利用所述加密字段替换所述数据报文的序列号中的第一字段，从而得到修改后的数据报文
304
第一网络设备向所述第二网络设备发送所述修改后的数据报文
305

图3

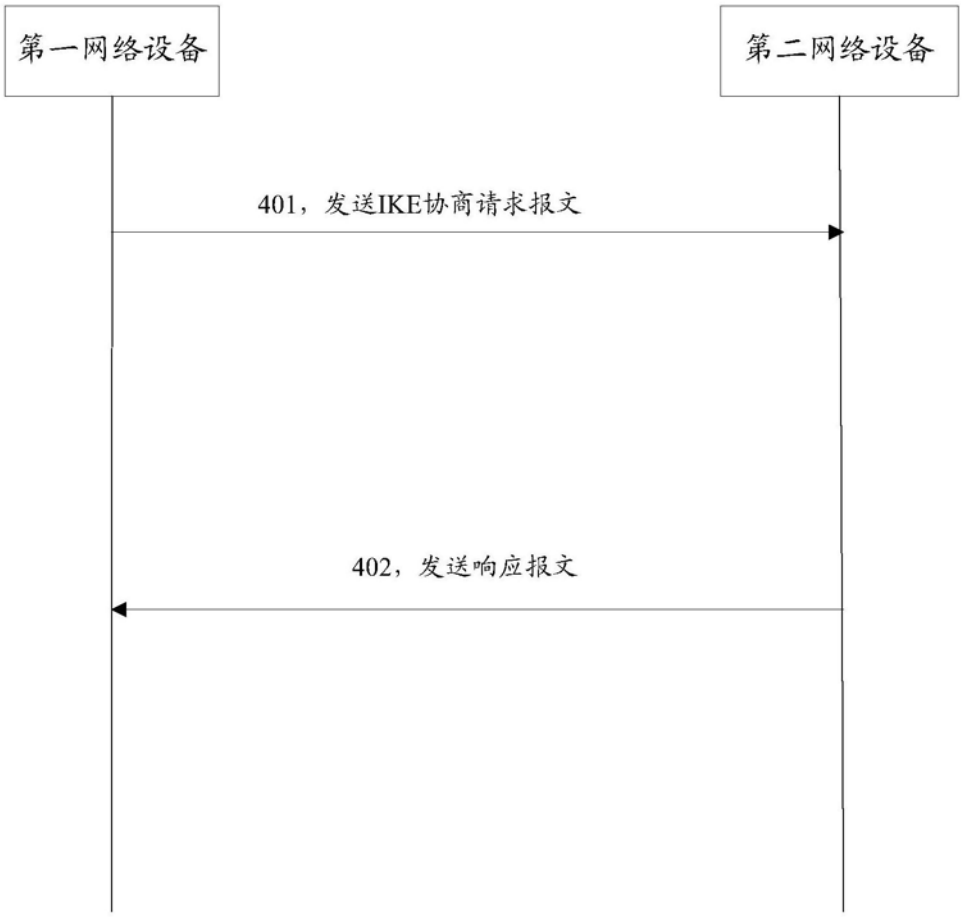

第一网络设备
第二网络设备
401，发送IKE协商请求报文
402，发送响应报文

图4

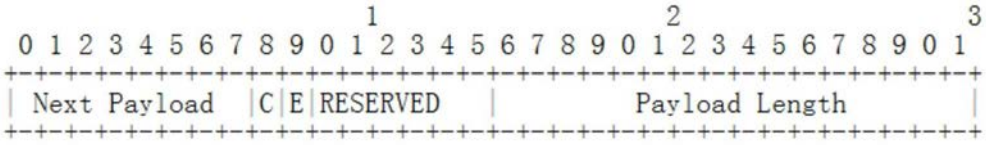

1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Payload
C
E
RESERVED
Payload Length

图5a

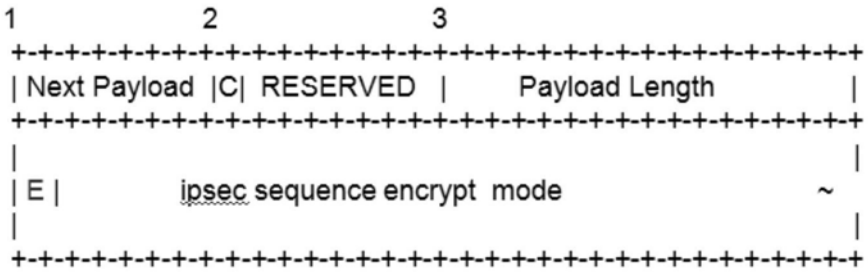

1 2 3
Next Payload
C
RESERVED
Payload Length
E
ipsec sequence encrypt mode

图5b

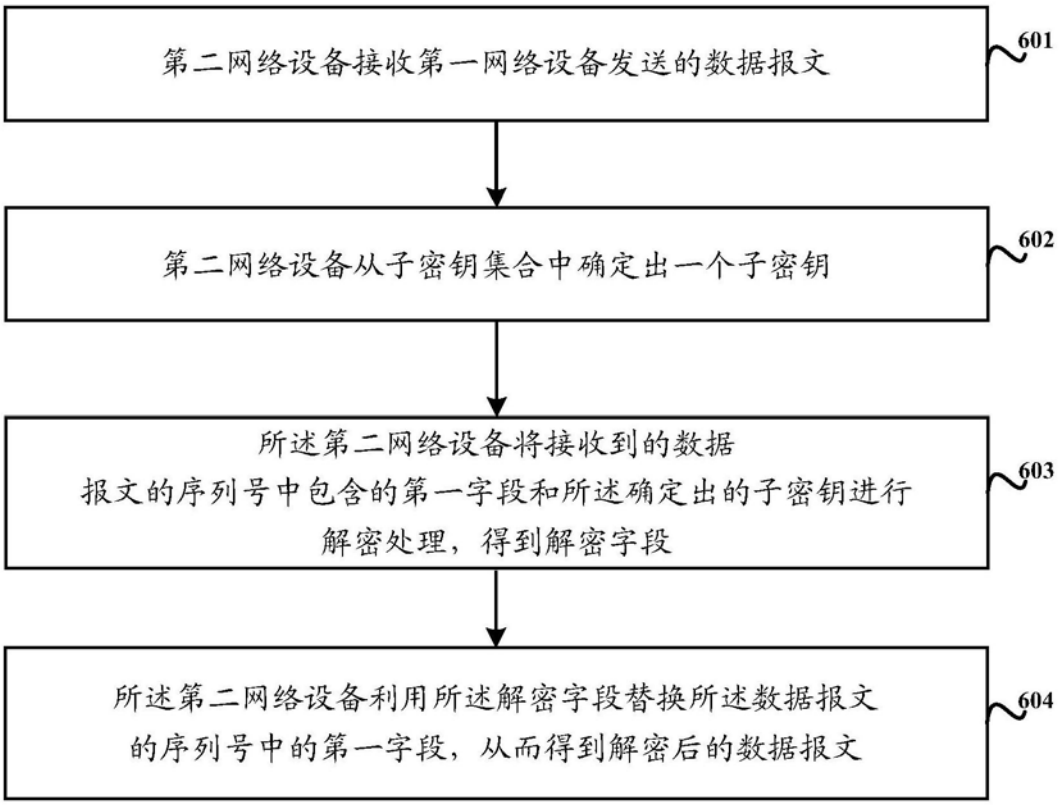

第二网络设备接收第一网络设备发送的数据报文
601
第二网络设备从子密钥集合中确定出一个子密钥
602
所述第二网络设备将接收到的数据报文的序列号中包含的第一字段和所述确定出的子密钥进行解密处理，得到解密字段
603
所述第二网络设备利用所述解密字段替换所述数据报文的序列号中的第一字段，从而得到解密后的数据报文
604

图6

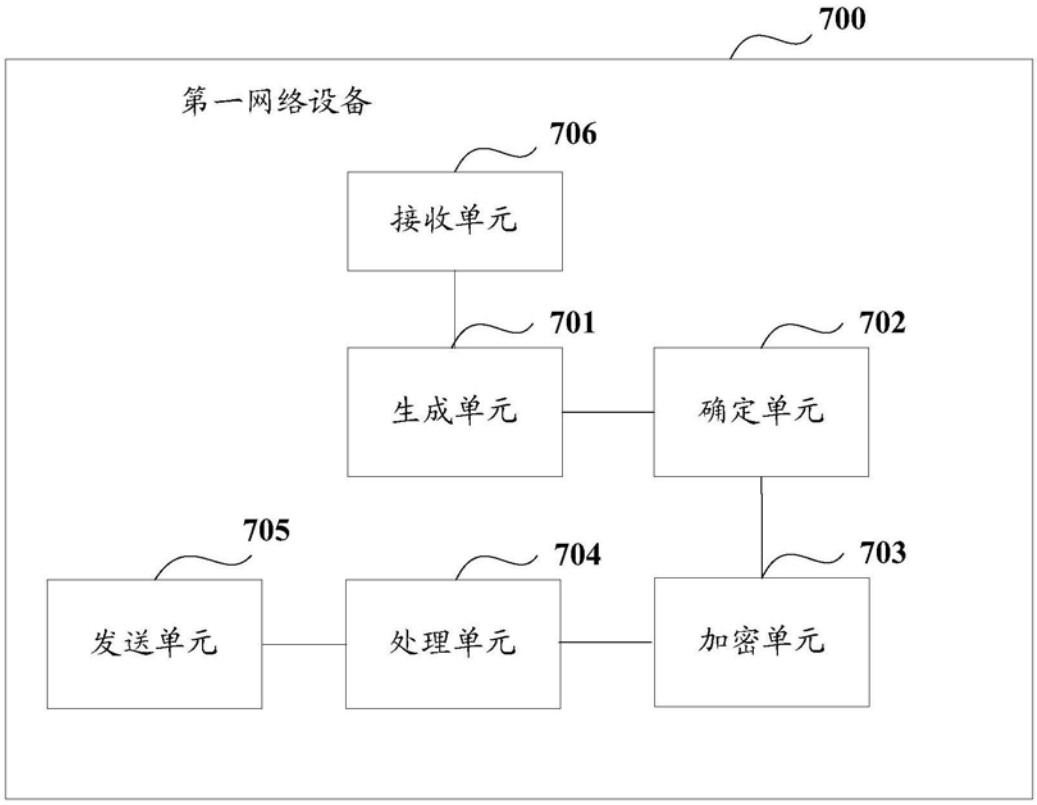

700
第一网络设备
706
接收单元
701
生成单元
702
确定单元
705
发送单元
704
处理单元
703
加密单元

图7

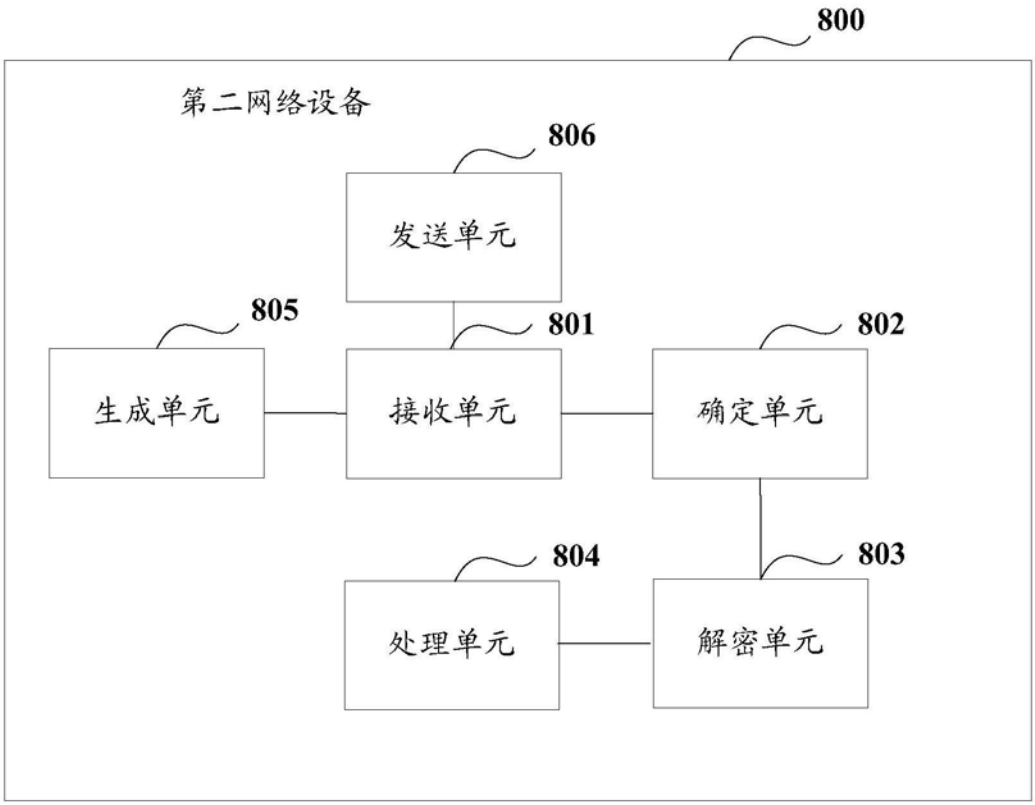

800
第二网络设备
806
发送单元
805
801
802
生成单元
接收单元
确定单元
804
803
处理单元
解密单元

图8

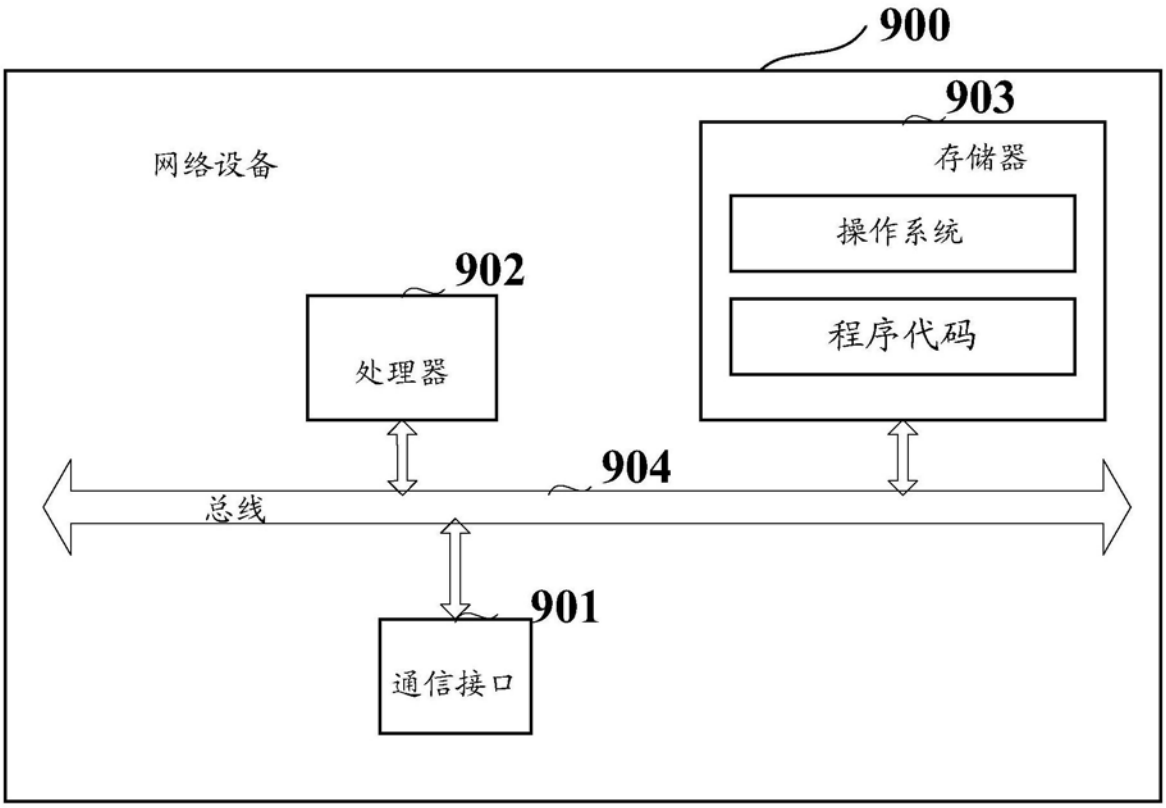


图9